

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Optical Media Protection Methods and Apparatuses**

Inventors:

**Darko Kirovski**

## **TECHNICAL FIELD**

The present invention relates generally to optical media and related devices, and more particularly to improved optical media and methods and apparatuses related thereto.

## **BACKGROUND**

Optical data storage media, such as, for example, compact discs and digital versatile discs are used to share a wide variety of data content. Music, movies and software are prime examples of the type of data one finds on individually-recorded and mass produced optical discs.

With the proliferation of such media and reading and writing devices there is a need to manage the digital and other rights that certain entities have in the recorded content on the discs. While data protection schemes have been used, there is, unfortunately, a thriving illegal data piracy market to which many of data protection schemes have fallen due to hacking efforts. Moreover, many of the protection schemes that have been used needed to only be broken once by a hacker who then shares the learned secrets of the protection scheme with others.

Consequently, there is a continuing need for improved methods and apparatuses for use in protecting data content stored on optical data storage media.

## **SUMMARY**

The above-stated needs and others are met, for example by an improved optical data storage medium is that has instructional data for an optical media content protection scheme built-in. The instructional data (e.g., software) is configured to cause programmable logic within the reading device to operatively

1 perform in accordance with the content protection scheme and to control access to  
2 the content data stored on the optical data storage medium accordingly. The  
3 content protection scheme may include, for example, a digital rights management  
4 (DRM) protection scheme, a marking scheme (e.g., a data-implemented water  
5 marking scheme, a data-implemented forensic marking scheme, etc.), and/or other  
6 like schemes.

7       The instructional data and/or the entire optical data storage medium can be  
8 verified based on at least one optically-detectable authentication feature and  
9 related information stored on the storage medium. Here, for example, the  
10 optically-detectable authentication feature may include a plurality of optically-  
11 detectable authentication features forming a substantially unique pattern using at  
12 least one optically detectable material. In certain implementations, such  
13 authentication features form an optically-detectable certificate of authentication  
14 (COA) that can be “read” and compared to related COA information data stored  
15 on the storage medium.

16       In accordance with certain implementations, another improved optical data  
17 storage medium is provided that includes optically-readable material suitable for  
18 storing data therein, and at least one optically-detectable non-data-based, physical  
19 authentication feature having a substantially unique pattern and comprising at least  
20 one optically detectable material.

21       An exemplary apparatus includes a means for storing instructional data for  
22 an optical media content protection scheme within an optical data storage medium,  
23 the instructional data being configured to cause logic associated with an optical  
24 media receiving device to operate in accordance with the optical media content  
25

1 protection scheme when programmed using the instructional data and accessing  
2 associated content data stored on the optical data storage medium.

3 Another exemplary apparatus includes a means for forming at least one  
4 optically-detectable non-data-based, physical authentication feature as part of an  
5 optical data storage medium, the authentication feature having a substantially  
6 unique pattern and comprising at least one optically detectable material.

7 Yet still another apparatus includes a data storage device that is  
8 configurable to write data to an optical data storage medium, and logic configured  
9 to cause the data storage device to record instructional data for an optical media  
10 content protection scheme within the optical data storage medium. Here, the  
11 instructional data is configured to cause logic associated with an optical media  
12 receiving device to operate in accordance with the optical media content  
13 protection scheme when programmed using the instructional data and accessing  
14 associated content on the an optical data storage medium.

15 Another apparatus includes an authentication feature forming mechanism  
16 configured to apply authentication feature forming material to an optical data  
17 storage medium so as to form at least one optically-detectable non-data-based,  
18 physical authentication feature as part of the optical data storage medium. Here,  
19 the authentication feature has a substantially unique pattern and is made using at  
20 least one optically detectable material.

21 In another exemplary method, instructional data is stored for an optical  
22 media content protection scheme within an optical data storage medium. The  
23 instructional data is configured to cause logic associated with an optical media  
24 receiving device to operate in accordance with the optical media content  
25

1 protection scheme when programmed using the instructional data and accessing  
2 associated content data stored on the optical data storage medium.

3 In still another implementation, a method is provided that includes forming  
4 at least one optically-detectable non-data-based, physical authentication feature as  
5 part of an optical data storage medium. Here, the authentication feature has a  
6 substantially unique pattern.

7 A computer-readable medium is also provided. The computer-readable  
8 medium includes computer-implementable instructions for causing at least one  
9 processor to write instructional data for an optical media content protection  
10 scheme to an optical data storage medium. Here, the instructional data being  
11 configured to cause logic associated with an optical media receiving device to  
12 operate in accordance with the optical media content protection scheme when  
13 programmed using the instructional data and accessing associated content data  
14 stored on the optical data storage medium.

15 Another exemplary apparatus includes non-volatile memory, an interface  
16 mechanism and logic. The interface mechanism is suitable for receiving a  
17 removable optical data storage medium, accessing instructional data associated  
18 with an optical media content protection scheme from the optical data storage  
19 medium, and outputting the accessed instructional data. The logic is operatively  
20 coupled to the interface mechanism and the non-volatile memory and configured  
21 to receive the accessed instructional data and in response thereto update a current  
22 optical media content protection scheme stored in the non-volatile memory and  
23 thereafter while accessing associated content data stored on the optical data  
24 storage medium operatively adhere to the updated current optical media content  
25 protection scheme.

1 A different apparatus includes an interface mechanism and logic. Here, an  
2 interface mechanism suitable for receiving a removable optical data storage  
3 medium, accessing and outputting data stored thereon, and detecting at least one  
4 optically-detectable authentication feature that is part of the optical data storage  
5 medium and outputting corresponding authentication feature information. The  
6 logic is operatively coupled to the interface mechanism and configured to receive  
7 the accessed data and the authentication feature information and in response  
8 thereto determine if content data stored on the optical data storage medium can be  
9 accessed.

10 Another method includes reading instructional data associated with an  
11 optical media content protection scheme from an optical data storage medium,  
12 updating a current optical media content protection scheme based on the  
13 instructional data, and determining if a valid license exists prior to accessing  
14 associated content data stored on the optical data storage medium.

15 Certain other methods include receiving a removable optical data storage  
16 medium, detecting at least one optically-detectable authentication feature that is  
17 part of the optical data storage medium, outputting authentication feature  
18 information, and determining if content data stored on the optical data storage  
19 medium can be accessed based at least in part on the authentication feature  
20 information.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

A more complete understanding of the various methods and apparatuses of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

Fig. 1 is a block diagram that depicts an exemplary system that can be used with and/or to form improved optical media, the device in this example takes the form of a computer.

Fig. 2 is a block diagram depicting an exemplary system for use with the improved optical media; the arrangement may include a computer and/or other types of devices/appliances.

Fig. 3 is a block diagram depicting certain exemplary aspects of the improved optical media suitable for use with the systems in Figs 1 and 2, and other like systems/devices.

Figs. 4(a-c) are illustrative cross-sectional diagrams depicting certain features of the improved optical media as in Fig. 3, for example.

Fig. 5 is a block diagram depicting a device as in Fig. 2, for example, for use with the improved optical media of Fig. 3.

Fig. 6 is a flow diagram depicting certain exemplary acts associated with a method for creating an improved optical media as in Fig. 3, for example.

Fig. 7 is a flow diagram depicting certain exemplary acts associated with a method for using an improved optical media as in Fig. 3, for example.

Fig. 8 is a block diagram depicting certain exemplary functions associated with the creation and usage of an improved optical media as in Fig. 3, for example.

1        Fig. 9 is a block diagram of a representative apparatus configured to create  
2        optically detectable certificate of authenticity (COA) features on improved optical  
3        media as in Figs. 3-4, for example.

4        Fig. 10 is an illustrative diagram depicting a conventional optical media in  
5        the form of a disc.

6        Figs. 11(a-c) are some illustrative diagrams depicting exemplary improved  
7        optical media in the form of discs.

### 8 9        **DETAILED DESCRIPTION**

10        Turning to the drawings, wherein like reference numerals refer to like  
11        elements, the invention is illustrated as being implemented in a suitable computing  
12        environment. Although not required, the invention will be described in the general  
13        context of computer-executable instructions, such as program modules, being  
14        executed by a personal computer. Generally, program modules include routines,  
15        programs, objects, components, data structures, etc. that perform particular tasks  
16        or implement particular abstract data types. Moreover, those skilled in the art will  
17        appreciate that the invention may be practiced with other computer system  
18        configurations, including hand-held devices, multi-processor systems,  
19        microprocessor based or programmable consumer electronics, network PCs,  
20        minicomputers, mainframe computers, and the like. The invention may also be  
21        practiced in distributed computing environments where tasks are performed by  
22        remote processing devices that are linked through a communications network. In  
23        a distributed computing environment, program modules may be located in both  
24        local and remote memory storage devices.



1 Fig.1 illustrates an example of a suitable computing environment 120 on  
2 which the subsequently described methods and apparatuses may be implemented.

3 Exemplary computing environment 120 is only one example of a suitable  
4 computing environment and is not intended to suggest any limitation as to the  
5 scope of use or functionality of the improved methods and apparatuses described  
6 herein. Neither should computing environment 120 be interpreted as having any  
7 dependency or requirement relating to any one or combination of components  
8 illustrated in computing environment 120.

9 The improved methods and apparatuses herein are operational with  
10 numerous other general purpose or special purpose computing system  
11 environments or configurations. Examples of well known computing systems,  
12 environments, and/or configurations that may be suitable include, but are not  
13 limited to, personal computers, server computers, thin clients, thick clients, hand-  
14 held or laptop devices, multiprocessor systems, microprocessor-based systems, set  
15 top boxes, programmable consumer electronics, network PCs, minicomputers,  
16 mainframe computers, distributed computing environments that include any of the  
17 above systems or devices, and the like.

18 As shown in Fig. 1, computing environment 120 includes a general-purpose  
19 computing device in the form of a computer 130. The components of computer  
20 130 may include one or more processors or processing units 132, a system  
21 memory 134, and a bus 136 that couples various system components including  
22 system memory 134 to processor 132.

23 Bus 136 represents one or more of any of several types of bus structures,  
24 including a memory bus or memory controller, a peripheral bus, an accelerated  
25 graphics port, and a processor or local bus using any of a variety of bus

1 architectures. By way of example, and not limitation, such architectures include  
2 Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA)  
3 bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA)  
4 local bus, and Peripheral Component Interconnects (PCI) bus also known as  
5 Mezzanine bus.

6 Computer 130 typically includes a variety of computer readable media.  
7 Such media may be any available media that is accessible by computer 130, and it  
8 includes both volatile and non-volatile media, removable and non-removable  
9 media.

10 In Fig. 1, system memory 134 includes computer readable media in the  
11 form of volatile memory, such as random access memory (RAM) 140, and/or non-  
12 volatile memory, such as read only memory (ROM) 138. A basic input/output  
13 system (BIOS) 142, containing the basic routines that help to transfer information  
14 between elements within computer 130, such as during start-up, is stored in ROM  
15 138. RAM 140 typically contains data and/or program modules that are  
16 immediately accessible to and/or presently being operated on by processor 132.

17 Computer 130 may further include other removable/non-removable,  
18 volatile/non-volatile computer storage media. For example, Fig. 1 illustrates a  
19 hard disk drive 144 for reading from and writing to a non-removable, non-volatile  
20 magnetic media (not shown and typically called a "hard drive"), a magnetic disk  
21 drive 146 for reading from and writing to a removable, non-volatile magnetic disk  
22 148 (e.g., a "floppy disk"), and an optical disk drive 150 for reading from or  
23 writing to a removable, non-volatile optical disk 152 such as a CD-ROM, CD-R,  
24 CD-RW, DVD-ROM, DVD-RAM or other optical media. Hard disk drive 144,  
25

1 magnetic disk drive 146 and optical disk drive 150 are each connected to bus 136  
2 by one or more interfaces 154.

3 The drives and associated computer-readable media provide nonvolatile  
4 storage of computer readable instructions, data structures, program modules, and  
5 other data for computer 130. Although the exemplary environment described  
6 herein employs a hard disk, a removable magnetic disk 148 and a removable  
7 optical disk 152, it should be appreciated by those skilled in the art that other types  
8 of computer readable media which can store data that is accessible by a computer,  
9 such as magnetic cassettes, flash memory cards, digital video disks, random access  
10 memories (RAMs), read only memories (ROM), and the like, may also be used in  
11 the exemplary operating environment.

12 A number of program modules may be stored on the hard disk, magnetic  
13 disk 148, optical disk 152, ROM 138, or RAM 140, including, e.g., an operating  
14 system 158, one or more application programs 160, other program modules 162,  
15 and program data 164.

16 The improved methods and apparatuses described herein may be  
17 implemented within operating system 158, one or more application programs 160,  
18 other program modules 162, and/or program data 164.

19 A user may provide commands and information into computer 130 through  
20 input devices such as keyboard 166 and pointing device 168 (such as a "mouse").  
21 Other input devices (not shown) may include a microphone, joystick, game pad,  
22 satellite dish, serial port, scanner, camera, etc. These and other input devices are  
23 connected to the processing unit 132 through a user input interface 170 that is  
24 coupled to bus 136, but may be connected by other interface and bus structures,  
25 such as a parallel port, game port, or a universal serial bus (USB).

1 A monitor 172 or other type of display device is also connected to bus 136  
2 via an interface, such as a video adapter 174. In addition to monitor 172, personal  
3 computers typically include other peripheral output devices (not shown), such as  
4 speakers and printers, which may be connected through output peripheral interface  
5 175.

6 Computer 130 may operate in a networked environment using logical  
7 connections to one or more remote computers, such as a remote computer 182.  
8 Remote computer 182 may include many or all of the elements and features  
9 described herein relative to computer 130.

10 Logical connections shown in Fig. 1 are a local area network (LAN) 177  
11 and a general wide area network (WAN) 179. Such networking environments are  
12 commonplace in offices, enterprise-wide computer networks, intranets, and the  
13 Internet.

14 When used in a LAN networking environment, computer 130 is connected  
15 to LAN 177 via network interface or adapter 186. When used in a WAN  
16 networking environment, the computer typically includes a modem 178 or other  
17 means for establishing communications over WAN 179. Modem 178, which may  
18 be internal or external, may be connected to system bus 136 via the user input  
19 interface 170 or other appropriate mechanism.

20 Depicted in Fig. 1, is a specific implementation of a WAN via the Internet.  
21 Here, computer 130 employs modem 178 to establish communications with at  
22 least one remote computer 182 via the Internet 180.

23 In a networked environment, program modules depicted relative to  
24 computer 130, or portions thereof, may be stored in a remote memory storage  
25 device. Thus, e.g., as depicted in Fig. 1, remote application programs 189 may

1 reside on a memory device of remote computer 182. It will be appreciated that the  
2 network connections shown and described are exemplary and other means of  
3 establishing a communications link between the computers may be used.

4 Attention is now drawn to Fig. 2, which is a block diagram depicting an  
5 exemplary arrangement/system for use with the improved optical media as  
6 described herein. This arrangement may include, for example, a computer as in  
7 Fig. 1 and/or other types of devices/appliances. The methods and apparatuses  
8 herein are not limited to computer or other like devices, and are clearly adaptable  
9 to any device or system that uses optical data storage media. As used herein an  
10 optical data storage medium may take any applicable form, and may include  
11 conventional forms, such as, for example, a compact disc (CD), a CD-ROM, a  
12 CD-R, a CD+R, a CD-RW, a CD+RW, a writable CD, a re-writable CD, a digital  
13 versatile disc (DVD), a DVD-RAM, a DVD-ROM, a DVD-R, a DVD+R, a DVD-  
14 RW, a DVD+RW, a writable DVD, a re-writable DVD, a laser disc, a non-disc  
15 optically-readable data storage medium, and/or the like.

16 Turning to Fig. 2, exemplary arrangement 200 includes an optical data  
17 storage medium (optical media) 202, a device 204, an external system 206 and a  
18 system 208. As mentioned above optical media 202 may take various forms.  
19 Device 204 is representative of any applicable device that is configured to  
20 interface with optical media 202. Thus, for example, device 204 may take the  
21 form of a CD or DVD player/reader/writer, etc. At a minimum, however, device  
22 204 is configured to read data stored on optical media 202. System 208 may  
23 include, for example, a computer, stereo, television, etc., having a device 204  
24 therein.

1 External system 206 is illustrative of potential exemplary implementations  
2 wherein device 204 may be remote to other devices/systems. Hence, for example,  
3 device 204 may be connected to external system 206 via a network, wireless link,  
4 etc. Logic within device 204 may interact with logic within external system 206  
5 through such connections. One example, is where external system 206 is  
6 operatively involved in helping device 204 and/or system 208 to determine if  
7 certain digital rights management (DRM), copyright or other like licenses exist for  
8 a given user, device, medium, content, period of time, etc. External device 206  
9 may support the distribution of cryptography related information, such as, e.g.,  
10 distribution of private and public keys, authenticating users, accounts, and the like.  
11 Here, external system 206 may include a “trusted source”, for example.

12 Fig. 3 is a block diagram depicting certain exemplary aspects of the  
13 improved optical media 202 suitable for use with the systems in Figs 1 and 2, and  
14 other like systems/devices.

15 Optical media 202 includes header information 302, media/content  
16 protection software 304, content 306, and optically-detectable certificate of  
17 authentication (COA) feature(s) 308. Header 302 includes, in this example, media  
18 identification information 310, license information 312, and COA information  
19 314. Header 302 is configured to convey to device 204, which sections/portions  
20 of optical media 202 include content 306 and protection software 304. ID  
21 information 310 can be included to uniquely or substantially uniquely identify  
22 optical media 202. License information 312 provides information about DRM or  
23 other like licenses/licensing applicable to the media itself and/or content 306.  
24 COA information 314 provides additional information associated with a COA  
25 feature as needed.

1 COA feature 308 is representative of an optically detectable feature that is  
2 unique or at least substantially unique to optical media 202. COA feature 308 in  
3 certain implementations includes one or more features that are optically detectable  
4 by device 204. COA feature 308 need not be a traditional optical data recording.  
5 Indeed, as described in greater detail below, COA 308 may include hardened  
6 plastic or epoxy droplets that are applied to a portion of optical media 202 and  
7 detectable using conventional and/or special purpose optical emission/detection  
8 circuitry (e.g., lasers, LEDs, related circuitry, etc.).

9 One basic desire is to have COA feature 308 substantially unique and  
10 robust enough so as to allow device 204 to detect it and, based on information  
11 collected about it during detection, determine if optical media 202 is  
12 authentic/verified in some way. This determination may then be used to increase  
13 confidence in media 202 and/or data stored thereon, control access to content 306,  
14 support other trust-based processes, improved DRM schemes, etc.

15 With this in mind, Figs. 4(a-c) are illustrative cross-sectional diagrams  
16 depicting certain exemplary types or arrangements of COA features 308. In Fig.  
17 4(a) optical media 202 includes a COA feature 308' having one or more optically-  
18 detectable features 402 that are formed on a surface of optical media 202. This  
19 can be accomplished, for example, by spraying or otherwise applying droplets of  
20 plastic (e.g., polymer), epoxy, glue, paint, dye, or other type of opaque or partially  
21 opaque material to a portion of the top surface of optical media 202. In certain  
22 implementations it may also be possible to use an optically transparent material  
23 that results in an optically-detectable feature/interface. Fig. 4(b) depicts COA  
24 feature 308'' having one or more optically-detectable features 404 that are formed  
25 below the top surface of optical media 202. Features 404 may include, for

1 example, materials and/or topologies that are optically-detectable by device 204.  
2 Fig. 4(c) depicts COA feature 308''' having one or more optically-detectable  
3 features 406 that are formed so as to extend into at least a portion of the top  
4 surface of optical media 202. Features 406 may include, for example, materials  
5 and/or topologies that are optically-detectable by device 204. In certain  
6 implementations, for example, features 406 may include etched features that are  
7 optically detectable.

8 As illustrated in the examples in Fig. 4, COA features may include a variety  
9 of optically-detectable features. When it is desired that COA feature 308 be  
10 unique or substantially unique, and/or otherwise difficult to copy or reproduce,  
11 then the pattern and/or shape of the feature may be randomly produced by  
12 spraying, misting, splattering, etc., some material in liquid form.

13 By way of example, techniques developed in the Cold War to track and  
14 account for nuclear warheads and missiles can be adapted for use in forming COA  
15 feature 308. Inspectors developed a technique for verifying each item that was  
16 tracked as part of treaties by spraying an area of the item with an epoxy. Once  
17 hardened, a photographic image was taken of the epoxy spray pattern.  
18 Subsequently taken photographs were then visually compared (e.g., a negative to  
19 positive comparison) to determine if the item had been altered or switched. It is  
20 believed that replicating such a random spray pattern and resulting hardened  
21 droplets would be significantly difficult if not impossible given that the optical  
22 reflection produced by the pattern and captured by the photographs at different  
23 times are being carefully compared.

24 This type of idea is adapted to optical data storage mediums in accordance  
25 with certain implementations. Rather than requiring human interaction and visual



1 photographic analysis, COA feature 308 are designed to be detected by device 204  
2 using conventional light emitting and detecting circuitry techniques. Thus, for  
3 example, the output of an LED or a laser may be directed towards COA feature  
4 308 and light detectors employed to determine reflected light levels/etc. (or lack  
5 thereof) returning from COA feature 308 and/or surrounding regions.

6 Features 402, 404 and/or 406 and others like them can be formed during the  
7 manufacture of optical media 202. For example, attention is drawn to Fig. 9,  
8 which illustrates a system 900 having a COA feature forming mechanism 902 that  
9 controls the application of a COA feature forming material 904 to optical media  
10 202. Those skilled in the art will recognize that the application of COA feature  
11 forming material 904 may occur in a variety of ways depending on the material,  
12 temperature, location on media 202, etc. Note that in certain implementations  
13 COA feature forming material 904 may add material to media 202, change  
14 material that is part of media 202, and/or cause material in media 202 to be  
15 removed. In certain implementations, COA feature forming material 904 may  
16 include liquid and/or solid materials applied separately or together and or at  
17 varying temperatures.

18 Attention is drawn next to Fig. 5, which is a block diagram depicting an  
19 exemplary implementation of device 204 in greater detail. Device 204 includes  
20 device logic 502, which in this example, includes a controller 504 and marking  
21 technology logic 506. Controller 504 may include a central processing unit (CPU)  
22 or like programmable logic. Marking technology 506 includes logic that used to  
23 support marking or other types of DRM, copyright protection, processes and the  
24 like.

1 As shown, device logic 502 is operatively coupled to RAM 508 and non-  
2 volatile memory 510 in this example. RAM 508 is used, for example, to support  
3 reading and writing processes associated with optical media 202. Non-volatile  
4 memory 510 is employed to persist data storage associated with protection  
5 software 304, license 312 and other similar processes that are part of the protection  
6 or DRM scheme provided by device 204 and/or optical media 202. In certain  
7 examples, non-volatile memory 510 include FLASH memory, SRAM, etc., that is  
8 configured to maintain information such as updatable protection software 512  
9 and/or license/usage information 514. Thus, for example, device logic 502 can be  
10 programmed using information (e.g., the data, instructions, etc.) stored in non-  
11 volatile memory 510 and device logic 502 can update information stored in non-  
12 volatile memory 510 based on protection software 304, header 302, COA feature  
13 308, and/or content 306, as applicable to support adherence to a desired/required  
14 DRM scheme.

15 Device logic 502 is also operatively coupled to an optical media interface  
16 mechanism 516, which is illustrated in this exemplary implementation as having at  
17 least one read head 518. Read head 518 is representative of the circuitry and  
18 mechanism that allows for the reading of data stored on optical media 202 and also  
19 for the detection of COA feature 308, if applicable. Read head technology is well-  
20 known. In certain implementations, multiple read heads 518 may be used; this too  
21 is well-known. Optical media interface mechanism 516 may also include one or  
22 more write heads 520. In certain implementations, read and write head technology  
23 may be combined into one unit. Also included in optical media interface  
24 mechanism 516 is an optical media mechanical movement unit 522, which is  
25 configured to receive, move (as necessary), and eject optical media 202

1 accordingly. Thus, for example, optical media mechanical movement unit 522  
2 may include a tray, holder, spindle motor, etc., as needed to handle optical media  
3 202. Again, such technologies are well-known.

4 Fig. 6 depicting certain exemplary acts associated with a method 600 for  
5 creating an improved optical media as in Fig. 3, for example. In act 602, a COA  
6 feature 318 is created, for example, as previously described. Next, in act 604, the  
7 COA feature created in act 602 is optically detected or “read” in a manner that  
8 produces information (here, e.g., a signal and/or data) corresponding to the  
9 detected/observed optical/light reflective properties of COA feature 318. The raw  
10 COA information (e.g., plaintext) data in act 604 may be gathered, for example, by  
11 a read head passing COA feature 318.

12 In act 606, all or part of the information from act 604 is used to generate a  
13 corresponding COA feature signature. Act 606, for example, in certain  
14 implementations and as described in greater detail below uses cryptographic  
15 algorithms to generate the COA feature signature. Next, in act 608, COA  
16 information 314 is recorded or otherwise stored to optical media 202. In certain  
17 implementations, for example, COA information 314 may include the COA feature  
18 signature from act 606 and the plaintext from act 604. In act 610, if optical media  
19 202 is to include updated protection software 304, then this is also recorded or  
20 otherwise stored in optical media 202. In act 612, content data 306 is recorded or  
21 otherwise stored to optical media 202.

22 Note that the acts in method 600 may be rearranged accordingly. Also, it  
23 should be recognized that while in certain implementations data may be written to  
24 the optical medium, for example, using a write head, in other implementations the  
25

1 optical medium may be manufactured to have data already stored thereon. These  
2 techniques and others like them are also well-known.

3 Fig. 7 depicts certain exemplary acts associated with a method 700 for  
4 using an improved optical media as in Fig. 3, for example. Here, in act 702, COA  
5 information 314 is read. In act 704 the COA information is verified. Act 702  
6 essentially, verifies that the COA information is valid. An example of a  
7 verification process is described and shown below with regard to Fig. 8.

8 Next, in act 706, COA feature 318 is “read”, and in act 708 the COA feature  
9 is verified. In the example, of Fig. 8, the verification of the COA feature is based  
10 on a comparison to part of the verified COA information.

11 With the verification in acts 704 and 706 satisfied, then in act 710, any  
12 update to protection software 304/512 is completed. Then, with the current  
13 updated protection software operating, in act 712, any license(s) required for  
14 accessing/processing the desired content 306 can be verified or otherwise handled.  
15 Act 712, for example, may include adding or modifying license/usage information  
16 514 in non-volatile memory 510 of device 204. Consequently, device logic 502  
17 may keep track of usage/access to content 306, and/or adhere to or enforce DRM  
18 or other like schemes as provided for in the protection software.

19 Attention is now drawn to Fig. 8, which is a block diagram depicting  
20 certain exemplary functions associated with the creation and usage of an improved  
21 optical media as in Fig. 3, for example. Arrangement 800 includes two sections  
22 that are illustrated as being above and below a dashed line. The functions above  
23 the dashed line would likely occur during manufacture of optical media 202 and  
24 the functions below the dashed line would likely occur during typical use of the  
25 resulting optical media. Note the not all data recording acts are depicted.

1 A COA feature read out 802 is performed (e.g., as in act 604). The  
2 resulting plaintext is included in COA information 314 and also provided to a hash  
3 function 804. Hash function 804 cryptographically hashes the plaintext to produce  
4 message " $m$ ". By way of example, hash function 804 (and hash function 818) may  
5 use a SHA1 or other like hash functions.

6 Message  $m$  is then processed using a decrypt function 806. In this example,  
7 decrypt function 806 uses a private key 808 associated with the digital rights  
8 holder, copyright holder, media manufacturer, publisher, user, and/or other  
9 applicable entity. In certain implementations, for example, decrypt function 806  
10 (and an encrypt function 810) may use RSA or other like cryptography techniques.  
11 The resulting signature from decrypt function 806 is included in COA information  
12 314.

13 Below the dashed line, when the optical medium is being initially read, the  
14 signature is accessed from COA information 314 and processed by encrypt  
15 function 810 to reproduce message " $m$ ". Here, for example, a public key  
16 corresponding to private key 808 may be used. The plaintext from COA  
17 information 314 is processed by a hash function 818 producing message " $m^*$ ". To  
18 verify that COA information 314 is authentic, a compare function 816 is  
19 performed with messages  $m$  and  $m^*$  as inputs. If messages  $m$  and  $m^*$  match  
20 (=true) per compare function 818, then COA information 314 is deemed verified  
21 in this example.

22 Having verified COA information, the COA feature can then be "read" and  
23 compared to the COA information. This is illustrated by a COA feature read out  
24 820, which produces plaintext\* as an output. Plaintext from COA information 314  
25 is then compared to plaintext\* in a compare function 822. If compare function

1 822 determines that plaintext and plaintext\* “match” (e.g., are sufficiently alike)  
2 then the verification of optical media 202 is complete and other processes may  
3 continue to consider license 312, or other like requirements, and/or proceed to  
4 access content 306.

5 Note that in certain implementations, it may be difficult to have an exact  
6 mathematical match occur in compare function 822 given the number of variables  
7 associated with “reading” certain types of COA features. Thus, in certain  
8 implementations, something less than an exact match may qualify as a “match”.  
9 For example, in certain implementations, a threshold-based or other like  
10 percentage-based matching/comparison function may be employed to allow for a  
11 certain level of deviation in the COA feature “read” data. In certain  
12 implementations, for example, a hamming distance threshold may be used.

13 Attention is now drawn to Fig. 10, which is an illustrative diagram  
14 depicting a conventional optical media in the form of a disc 1000. Disc 1000 may,  
15 for example, be a prior art CD, DVD, etc. Here, in this example, disc 1000  
16 includes spindle mounting hole 1002, a non-data region 1004, an indexing data  
17 region 1006, and a content data region 1008. Indexing data region 1006 is  
18 representative of any type of data/information that may be needed to identify the  
19 layout of disc 1000 and in particular the data in content data region 1008. Those  
20 skilled in the art will recognize that other regions and/or data may also be  
21 included, and that the exemplary layout shown in Fig. 10 is illustrative only and  
22 that an actual physical layout of such data/regions may take various forms as  
23 allowed under applicable standards/formats. Also, those skilled in the art will  
24 recognize that a block of data may be written/stored in one contiguous section on  
25

1 disc 1000 or in some manner sub divided and written/stored in a plurality of  
2 different sections on disc 1000.

3 Figs 11(a-c) are similar illustrative diagrams depicting certain exemplary  
4 improved optical media implementations in the form of discs 1100, 1100', and  
5 1100'', respectively. These are only a few illustrative examples.

6 In Fig. 11(a), for example, disc 1100 includes spindle mounting hole 1002,  
7 non-data region 1004, and indexing data region 1006. Disc 1100 also includes  
8 content 306. Header 302 is included within indexing data region 1006, in this  
9 example, with data as applicable to protection software 304, which is also included  
10 in disc 1100.

11 In Fig. 11(b), for example, disc 1100' also includes spindle mounting hole  
12 1002, non-data region 1004, and indexing data region 1006. Disc 1100' further  
13 includes content 306 and COA feature 308. Header 302 is also included within  
14 indexing data region 1006, in this example. Header 302 includes data applicable  
15 to COA feature 308.

16 In Fig. 11(c), for example, Disc 1100'' also includes spindle mounting hole  
17 1002, non-data region 1004, and indexing data region 1006. Disc 1100'' further  
18 includes content 306, protection software 304, and COA feature 308. Header 302  
19 is also included within indexing data region 1006, in this example. Here, header  
20 302 includes data applicable to protection software 304 and COA feature 308.

21 Although some preferred embodiments of the various methods and  
22 apparatuses of the present invention have been illustrated in the accompanying  
23 Drawings and described in the foregoing Detailed Description, it will be  
24 understood that the invention is not limited to the exemplary embodiments  
25 disclosed, but is capable of numerous rearrangements, modifications and

1 substitutions without departing from the spirit of the invention as set forth and  
2 defined by the following claims.

3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25